

Algebra & Number Theory

Volume 13
2019
No. 6

An improved bound for the lengths of matrix algebras

Yaroslav Shitov



An improved bound for the lengths of matrix algebras

Yaroslav Shitov

Let S be a set of $n \times n$ matrices over a field \mathbb{F} . We show that the \mathbb{F} -linear span of the words in S of length at most

$$2n \log_2 n + 4n$$

is the full \mathbb{F} -algebra generated by S . This improves on the $\frac{n^2}{3} + \frac{2}{3}$ bound by Paz (1984) and an $O(n^{3/2})$ bound of Pappacena (1997).

Let S be a subset of a finite-dimensional associative algebra \mathcal{A} over a field \mathbb{F} . An element $a \in \mathcal{A}$ is said to be a *word* of length k in S if there are $a_1, \dots, a_k \in S$ such that $a = a_1 \cdots a_k$. We denote the set of all such words by S^k , and we write $\mathbb{F}S^k$ for the \mathbb{F} -linear span of S^k . Similarly, $\mathbb{F}S^{\leq k}$ will stand for the \mathbb{F} -linear span of all the words in S that have length at most k .

Definition 1. The length $\ell(S)$ is the smallest integer k for which $\mathbb{F}S^{\leq k}$ is the full subalgebra generated by S . We also define $\ell(\mathcal{A})$ as the maximum value of $\ell(S)$, where S runs over all subsets of \mathcal{A} that generate \mathcal{A} as an \mathbb{F} -algebra.

In our paper, we study the length of $\text{Mat}_n(\mathbb{F})$, the set of $n \times n$ matrices viewed as an algebra over \mathbb{F} . A. Paz [1984] proved that $\ell(S) \leq \frac{n^2}{3} + \frac{2}{3}$ for all $S \subset \text{Mat}_n(\mathbb{F})$ and proposed the following appealing conjecture.

Conjecture 2. For all $S \subset \text{Mat}_n(\mathbb{F})$, one has $\ell(S) \leq 2n - 2$.

As shown by T. Laffey [1986, page 131], the upper bound in Conjecture 2 should be sharp. This conjecture is known to hold if the size of matrices is at most four [Paz 1984] or if $\mathbb{F}S$ contains a nonderogatory matrix [Guterman et al. 2018]. However, the best known general upper bounds on the lengths of matrix subsets are quite far from the one prescribed by Conjecture 2. It was only in 1997 when a subquadratic estimate was obtained: C. Pappacena proved an $O(n^{3/2})$ upper bound on the length of $\text{Mat}_n(\mathbb{F})$, but no further improvements have been made since then [Guterman et al. 2018; Lambrou and Longstaff 2009; Longstaff et al. 2006]. The main result of this paper is a much stronger $O(n \log n)$ upper bound on the length of $\text{Mat}_n(\mathbb{F})$.

Theorem 3. For all $S \subset \text{Mat}_n(\mathbb{F})$, we have $\ell(S) \leq 2n \log_2 n + 4n - 4$.

MSC2010: primary 15A03; secondary 15A30.

Keywords: matrix theory, finite-dimensional algebras, generating sets.

As an additional motivation of our study, we note that the best known upper bounds on a complete set of unitary invariants for $n \times n$ matrices [Laffey 1986] and on the PI degree of semiprime affine algebras of Gelfand–Kirillov dimension one [Pappacena et al. 2003] come from the estimates of $\ell(\text{Mat}_n(\mathbb{F}))$, so the current work also improves our understanding of those invariants.

1. Warm-up

In this section, we explain the idea behind our main construction and illustrate how it works in a simpler setting. We get a small improvement on one of the results of Pappacena [1997], which allows us to prove the $n = 5$ case of Conjecture 2.

We say that a set $S \subset \text{Mat}_n(\mathbb{F})$ is *irreducible* if it generates $\text{Mat}_n(\mathbb{F})$ as the \mathbb{F} -algebra. If a set S is not irreducible, and if \mathbb{F} is algebraically closed, then there exist $p \in \{1, \dots, n-1\}$ and $Q \in \text{GL}_n(\mathbb{F})$ such that, for any $A \in S$, we have

$$Q^{-1}AQ = \begin{pmatrix} A_{11} & A_{12} \\ O & A_{22} \end{pmatrix} \quad (1-1)$$

where A_{11} is a $p \times p$ matrix (and O is the zero matrix of appropriate dimensions). This is *Burnside's theorem*; see [Radjavi and Rosenthal 2000, Theorem 1.5.1].

Lemma 4 [Markova 2005, Corollary 3]. *Let \mathcal{A} be a matrix algebra whose elements are of the form (1-1), and let $\mathcal{A}_1, \mathcal{A}_2$ be the sets of all A_{11}, A_{22} blocks of matrices in \mathcal{A} , respectively. Then $\ell(\mathcal{A}) \leq \ell(\mathcal{A}_1) + \ell(\mathcal{A}_2) + 1$.*

We will say that a matrix $Z \in \text{Mat}_n(F)$ is *square-zero* if $Z^2 = 0$. The main idea of the proof of Theorem 3 is to control the product $\lambda\rho(\lambda)$, where $\rho(\lambda)$ is the minimal rank of nonzero square-zero matrices that arise as linear combinations of words of length at most λ . We show in Section 2 below that we can reduce ρ to 1 whilst saving the property $\lambda\rho(\lambda) \in O(n \log n)$, and then we apply Pappacena's technique to deal with low rank matrices; see [Pappacena 1997, Theorem 4.1] and Corollary 7 below. More precisely, let $H \in \mathbb{F}S^{\leq \lambda}$ be a square-zero matrix; it can be written as

$$H = \begin{pmatrix} O & O & I_\rho \\ O & O & O \\ O & O & O \end{pmatrix}$$

with respect to some basis. If some matrix A with bottom-left block of small rank $r > 0$ comes as a linear combination of words of length l , then the matrix $H A H$ is square-zero, has rank r , and comes as a linear combination of words of length at most $l + 2\lambda$. As we will see in Claims 13 and 14 below, we can always find an appropriate matrix A to reduce the rank of a square-zero matrix. The following lemma illustrates our approach to the proof of Claim 13.

Lemma 5. *Consider an irreducible set $S \subset \mathbb{F}^{n \times n}$ and a nonzero vector $v \in \mathbb{F}^n$. If $\mathbb{F}S^{\leq (n-2)}v \neq \mathbb{F}^n$, then $\mathbb{F}S$ contains a matrix with minimal polynomial of degree n .*

Proof. The sequence

$$\mathbb{F}v = \mathbb{F}S^0v \subset \mathbb{F}S^{\leq 1}v \subset \cdots \subset \mathbb{F}S^{\leq k}v = \mathbb{F}^n$$

is strictly increasing [Pappacena 1997, Theorem 4.1], so the assumption of the lemma implies $k = n - 1$ and $\dim \mathbb{F}S^{\leq t}v - \dim \mathbb{F}S^{\leq (t-1)}v = 1$ for all $t \in \{1, \dots, n - 1\}$. Therefore, we can set $\mathcal{B}_0 = \{v\}$ and inductively complete \mathcal{B}_{t-1} to a basis \mathcal{B}_t of $\mathbb{F}S^{\leq t}$ by adding a single vector v_t . With respect to the basis $\{v, v_1, \dots, v_{n-1}\}$, every matrix in S has the form

$$A = \begin{pmatrix} * & \cdots & \cdots & * & * \\ a_{21} & * & \cdots & * & * \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & * & * \\ 0 & \cdots & 0 & a_{n,n-1} & * \end{pmatrix}$$

with $*$'s denoting the entries we need not specify. Since S is irreducible, all of the $(i + 1, i)$ entries are nonzero at some matrix in S , so a generic element of $\mathbb{F}S$ has all of them nonzero — which means that its minimal polynomial has degree n . \square

Theorem 6 [Guterman et al. 2018, Theorems 2.4 and 2.5]. *If an irreducible set $\mathbb{F}S \subset \text{Mat}_n(\mathbb{F})$ contains a matrix with minimal polynomial of degree $n - 1$ or n , then $\ell(S) \leq 2n - 2$.*

Lemma 5 and Theorem 6 lead to a tiny improvement of the $r = 1$ case of Theorem 4.1(a) in [Pappacena 1997], which is nevertheless useful to study the case of small n .

Corollary 7. *Let $S \subset \text{Mat}_n(\mathbb{F})$ be an irreducible set and $k \geq 2$. If $\mathbb{F}S^{\leq k}$ contains a rank-one matrix, then $\ell(S) \leq 2n + k - 4$.*

Proof. If $\mathbb{F}S$ contains a matrix with minimal polynomial of degree n , then we are done by Theorem 6. Otherwise, we use Lemma 5 and get

$$\mathbb{F}S^{\leq (n-2)}AS^{\leq (n-2)} = \sum \text{Mat}_n(\mathbb{F}) \cdot A \cdot \text{Mat}_n(\mathbb{F}) = \text{Mat}_n(\mathbb{F})$$

for any rank-one matrix A . \square

We are almost ready to prove the $n = 5$ case of Conjecture 2.

Claim 8. *Assume that the minimal polynomial of every matrix in $\mathbb{F}S \subset \text{Mat}_n(\mathbb{F})$ has degree at most 2. Then $\ell(S) \leq 2 \log_2 n$.*

Proof. We denote by w a word in $S^{\ell(S)}$ that is not spanned by shorter words. For any $A, B \in S$, the matrices A^2 and $AB + BA = (A + B)^2 - A^2 - B^2$ belong to $\mathbb{F}S^{\leq 1}$, which implies that the letters of w are all different and their permutations do not break the property of w not to be spanned by shorter words. In particular, the products corresponding to the different $2^{\ell(S)}$ subsets of letters of w should be linearly independent, which implies $2^{\ell(S)} \leq \dim \text{Mat}_n(\mathbb{F})$. \square

Theorem 9. *If $S \subset \text{Mat}_5(\mathbb{F})$, then $\ell(S) \leq 8$.*

Proof. Since a set of vectors is linearly dependent over \mathbb{F} if it is linearly dependent over the algebraic closure of \mathbb{F} , it is sufficient to prove the statement assuming that \mathbb{F} is algebraically closed [Guterman et al. 2018, page 239]. Moreover, Conjecture 2 is known to hold for $n \leq 4$ (see [Paz 1984]), so we can use Lemma 4 and assume without loss of generality that S is irreducible. According to Theorem 6 and Claim 8, we can restrict to the case when $\mathbb{F}S$ contains a matrix A with minimal polynomial of degree 3. A straightforward analysis of possible Jordan forms of A shows that the linear span of I, A, A^2 must contain a rank-one matrix, so it remains to apply Corollary 7. \square

As said above, the case of $n \leq 4$ in Conjecture 2 was considered by Paz [1984], but the case of $n = 5$ remained open until now [Guterman et al. 2018]. Let us mention the works [Lambrou and Longstaff 2009; Longstaff et al. 2006], which cover the case $n \leq 6$ under the additional assumption of $\dim \mathbb{F}S \leq 2$.

2. The proof of Theorem 3

Let A be an $n \times n$ matrix over a field \mathbb{F} , which is assumed to be algebraically closed in this section. We recall that there exists $Q \in \mathrm{GL}_n(\mathbb{F})$ such that $Q^{-1}AQ$ has *rational normal form*, that is, we have $Q^{-1}AQ = \mathrm{diag}(C_{f_1}, \dots, C_{f_k})$, where

$$C_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{m-1} \end{pmatrix}$$

is the companion matrix of a polynomial $f = t^m + c_{m-1}t^{m-1} + \cdots + c_0$, and the *invariant factors* f_1, \dots, f_k satisfy $f_1 | \cdots | f_k$.

Claim 10. *Let δ be the degree of the minimal polynomial of an $n \times n$ matrix A over \mathbb{F} . Then the \mathbb{F} -linear span of $I, A, \dots, A^{\delta-1}$ contains either a nonzero projector of rank at most n/δ or a nonzero square-zero matrix of rank at most n/δ .*

Proof. We recall that the minimal polynomial φ of A occurs (one or more times) as an invariant factor of A . Let ψ be a polynomial that has degree $\delta - 1$, divides φ and is a multiple of any invariant factor different from φ . Then $\psi(A)$ has equal rank-one matrices in the places of the largest blocks of the rational normal form of A and zeros everywhere else. \square

Claim 11. *For any irreducible set $S \subset \mathrm{Mat}_n(\mathbb{F})$, there exist nonzero λ, ρ such that $\lambda\rho \leq 2n$ and $\mathbb{F}S^{\leq \lambda}$ contains a square-zero matrix of rank ρ .*

Proof. We apply Claim 10 to any nonscalar matrix in S and find a nonzero matrix $P \in \mathbb{F}S^{\leq (\delta-1)}$ that has rank at most n/δ and satisfies either $P^2 = P$ or $P^2 = 0$. We are done if $P^2 = 0$; otherwise $H_B = (I - P)BP$ is a square-zero matrix for all B . We can have $H_B = 0$ only when the columns of BP are in the kernel of $I - P$, but this kernel being equal to $\mathrm{Im} P$ should then be invariant with respect to B , but since S is irreducible, this obstruction cannot happen for all $B \in S$. \square

Claim 12. Let $A \in \mathbb{F}^{n \times n}$ and $r \in \mathbb{N}$. Assume that the inequality $\text{rank}(PAQ) \leq r$ holds, with any positive integers p, q , for all matrices $P \in \mathbb{F}^{p \times n}$, $Q \in \mathbb{F}^{n \times q}$ satisfying $PQ = 0$. Then $\text{rank}(A - \mu I) \leq 2r$ for some $\mu \in \mathbb{F}$.

Proof. Both the assumption and conclusion are independent of the substitution $A \rightarrow C^{-1}AC$, so we can assume that A has rational normal form. We denote the number of diagonal blocks by k and their sizes by m_1, \dots, m_k . Since the ranks of the diagonal blocks cannot decrease by more than one upon adding a scalar matrix, and since the characteristic polynomials of these blocks have a common factor, we have $\min_{\mu} \text{rank}(A - \mu I) = n - k$. We conclude the proof by constructing an identity square submatrix $A' = A[I|J]$ with $I \cap J = \emptyset$ and $|I| = |J| \geq 0.5(n - k)$, which would allow us to define P and Q as having the identity matrices at the $I \times I$ and $J \times J$ blocks and completed by an appropriate number of zero columns and rows, respectively. Namely, we pick a family of $\lfloor m_t/2 \rfloor$ nonconsecutive subdiagonal ones from a t -th diagonal block of A , and the union of all such families will be the diagonal of A' . \square

Claim 13. Let $S \subset \mathbb{F}^{n \times n}$, $P \in \mathbb{F}^{p \times n}$, $Q \in \mathbb{F}^{n \times q}$. Let k be the smallest integer such that $PS^kQ \neq 0$. Then, for any $A_1, \dots, A_k \in S$, we have $\text{rank}(PA_1 \cdots A_k Q) \leq n/k$.

Proof. Let $V_0 = \text{Im } Q$ and $V_t = \sum_{M \in S^{\leq t}} \text{Im } MQ$. Let $B_0, \dots, B_k \subset \mathbb{F}^n$ be vector families such that $B_0 \cup \dots \cup B_t$ is a basis of V_t for $t = 0, \dots, k$. Let $\mathcal{C} \subset \mathbb{F}^n$ be such that $B_0 \cup \dots \cup B_k \cup \mathcal{C}$ is a basis of \mathbb{F}^n . Every matrix $A \in S$ has the form

$$\begin{pmatrix} & B_0 & B_1 & \cdots & B_{k-1} & B_k & \mathcal{C} \\ B_0 & * & \cdots & \cdots & \cdots & * & * \\ B_1 & A(1, 0) & * & \cdots & \cdots & * & * \\ B_2 & O & A(2, 1) & * & \cdots & * & * \\ \vdots & \vdots & O & \ddots & * & \vdots & \vdots \\ B_k & \vdots & \vdots & \ddots & A(k, k-1) & * & * \\ \mathcal{C} & O & O & \cdots & O & * & * \end{pmatrix},$$

where the $*$'s stand for entries that we need not specify, and the left column and top row of the matrix above indicate the basis vectors the respective blocks of rows and columns correspond to. We also have $P = (O | \cdots | O | P' | *)$, $Q = (Q^\top | O | \cdots | O)^\top$ with some matrices P' , Q at the B_k position of P and the B_0 position of Q , respectively. For $A_1, \dots, A_k \in S$, the matrix $PA_k \cdots A_1 Q$ equals $P'A_k(k, k-1) \cdots A_1(1, 0)Q$, so its rank is at most the smallest dimension of any of the matrices $A_k(k, k-1), \dots, A_1(1, 0)$, which is $\min_t |B_t| \leq n/k$. \square

Claim 14. Let $S \subset \text{Mat}_n(\mathbb{F})$ be an irreducible set and assume that $\mathbb{F}S^{\leq \lambda}$ contains a square-zero matrix H of rank $\rho \geq 2$. Then there exist $\rho_1 \in [1, 0.5\rho]$ and

$$\lambda_1 \leq \frac{\lambda\rho}{\rho_1} + \frac{4n(\rho - \rho_1)}{\rho\rho_1}$$

such that $\mathbb{F}S^{\leq \lambda_1}$ contains a square-zero matrix of rank equal to ρ_1 .

Proof. Let $P \in \mathbb{F}^{p \times \rho}$, $Q \in \mathbb{F}^{\rho \times q}$ be nonzero matrices satisfying $PQ = 0$. We choose a basis such that

$$H = \begin{pmatrix} O & O & I_\rho \\ O & O & O \\ O & O & O \end{pmatrix}$$

and define $P' = (O|O|P)$ and $Q' = (Q^\top|O|O)^\top$. Let k be the smallest integer for which there exist p , q and matrices P' , Q' defined as above, and also $A_1, \dots, A_k \in S$ satisfying $P'A_1 \dots A_k Q' \neq 0$ (such an integer k exists because S is irreducible). We write $A = A_1 \dots A_k$, and we denote by A' the bottom left block of A . Since $PA'Q \neq 0$, the matrix A' is nonscalar, that is, its minimal polynomial has degree $\delta > 1$.

Case 1. Assume $k \leq 4n/\rho$. By [Claim 10](#), there is a polynomial ψ of degree at most $(\delta - 1)$ such that $\rho_1 := \text{rank } \psi(A') \in [1, \rho/\delta]$; we see that $H_1 = \psi(HA)H$ is a square-zero matrix of rank ρ_1 . It remains to note that H_1 is spanned by words of length at most

$$(\delta - 1)(\lambda + k) + \lambda \leq \lambda\delta + (\delta - 1)k \leq \lambda\rho/\rho_1 + 4n(\rho/\rho_1 - 1)/\rho.$$

Case 2. Now let $k \geq 4n/\rho$. The matrix HAH has A' at the upper right block and zeros everywhere else. According to [Claim 13](#), we have $\text{rank}(PA'Q) \leq n/k$ for any choice of p , q and P , Q as above. Using [Claim 12](#), we find a $\mu \in \mathbb{F}$ for which the matrix $H_1 := HAH - \mu H$ satisfies $\rho_1 := \text{rank}(H_1) \leq 2n/k$. So we have $\rho_1 \leq 0.5\rho$, and H_1 is spanned by words of length at most

$$2\lambda + k \leq \lambda\rho/\rho_1 + 2n/\rho_1 \leq \lambda\rho/\rho_1 + 4n(1 - \rho_1/\rho)/\rho_1. \quad \square$$

Proof of Theorem 3. As in the proof of [Theorem 9](#), we can assume without loss of generality that \mathbb{F} is algebraically closed and S is irreducible. Using [Claim 11](#), we find a square-zero matrix of rank $\rho_0 > 0$ in $\mathbb{F}S^{\leq \lambda_0}$ with $\lambda_0\rho_0 \leq 2n$; if $\rho_0 = 1$, then we apply [Corollary 7](#) and complete the proof. Otherwise, we repeatedly apply [Claim 14](#) and obtain a sequence $(\lambda_0, \rho_0), \dots, (\lambda_\tau, \rho_\tau)$ such that $\rho_\tau = 1$ and for all $t \in \{0, \dots, \tau - 1\}$ it holds that $\rho_{t+1} \in [1, 0.5\rho_t]$,

$$\lambda_{t+1} \leq \frac{\lambda_t \rho_t}{\rho_{t+1}} + \frac{4n(\rho_t - \rho_{t+1})}{\rho_t \rho_{t+1}},$$

and every $\mathbb{F}S^{\leq \lambda_t}$ contains a square-zero matrix of rank ρ_t . By induction we get

$$\lambda_t \leq \frac{\lambda_0 \rho_0}{\rho_t} + \frac{4n}{\rho_t} \left(t - \frac{\rho_1}{\rho_0} - \dots - \frac{\rho_t}{\rho_{t-1}} \right),$$

which implies (after the substitution $\alpha_t := \rho_t/\rho_{t-1}$) that

$$\lambda_\tau \leq 2n + 4n \left(\tau - \sum_{t=1}^{\tau} \alpha_t \right),$$

and since the minimum value of $\alpha_1 + \dots + \alpha_\tau$ subject to $\alpha_t > 0$ and $\alpha_1 \dots \alpha_\tau = \rho_0^{-1}$ is attained when $\alpha_1 = \dots = \alpha_\tau = \rho_0^{-1/\tau}$, we get

$$\lambda_\tau \leq 2n + 4n\tau(1 - \rho_0^{-1/\tau}).$$

The right-hand side of this inequality is an increasing function of τ , so it attains its maximum at the largest possible value $\tau = \log_2 \rho_0$. We get $\lambda_\tau \leq 2n + 2n \log_2 \rho_0$, and it remains to apply [Corollary 7](#). \square

The author does not expect his result to be tight even asymptotically, so this paper does not show any effort on improving the $o(n \log n)$ part of the upper bound.

Acknowledgments

The author is indebted to O.V. Markova from Moscow State University for a series of talks on the topic, which he has had a privilege to attend since 2006. Mateusz Michałek told the author in June 2018 about a very similar problem, known as the quantum version of Wielandt’s inequality [[Sanz et al. 2010](#)], and we quickly came to a conclusion that the progress on one of these problems can lead to the progress on the other. In particular, we managed [[Michałek and Shitov 2019](#)] to get an $O(n^2 \log n)$ bound for the largest value of τ such that the equality $\mathbb{F}S^\tau = \text{Mat}_n(\mathbb{F})$ holds for any set S for which there exists a t satisfying $\mathbb{F}S^t = \text{Mat}_n(\mathbb{F})$ — while the present paper gives an $O(n \log n)$ bound for the same problem but with S^τ , S^t replaced by $S^{\leq \tau}$, $S^{\leq t}$, respectively.

References

- [Guterman et al. 2018] A. Guterman, T. Laffey, O. Markova, and H. Šmigoc, “A resolution of Paz’s conjecture in the presence of a nonderogatory matrix”, *Linear Algebra Appl.* **543** (2018), 234–250. [MR](#) [Zbl](#)
- [Laffey 1986] T. J. Laffey, “Simultaneous reduction of sets of matrices under similarity”, *Linear Algebra Appl.* **84** (1986), 123–138. [MR](#) [Zbl](#)
- [Lambrou and Longstaff 2009] M. S. Lambrou and W. E. Longstaff, “On the lengths of pairs of complex matrices of size six”, *Bull. Aust. Math. Soc.* **80**:2 (2009), 177–201. [MR](#) [Zbl](#)
- [Longstaff et al. 2006] W. E. Longstaff, A. C. Niemeyer, and O. Panaia, “On the lengths of pairs of complex matrices of size at most five”, *Bull. Aust. Math. Soc.* **73**:3 (2006), 461–472. [MR](#) [Zbl](#)
- [Markova 2005] O. V. Markova, “On the length of the algebra of upper-triangular matrices”, *Uspekhi Mat. Nauk* **60**:5 (2005), 177–178. In Russian; translated in *Russ. Math. Surv.* **60**:5 (2005), 984–985. [MR](#) [Zbl](#)
- [Michałek and Shitov 2019] M. Michałek and Y. Shitov, “Quantum version of Wielandt’s inequality revisited”, *IEEE Trans. Inform. Theory* (online publication February 2019).
- [Pappacena 1997] C. J. Pappacena, “An upper bound for the length of a finite-dimensional algebra”, *J. Algebra* **197**:2 (1997), 535–545. [MR](#) [Zbl](#)
- [Pappacena et al. 2003] C. J. Pappacena, L. W. Small, and J. Wald, “Affine semiprime algebras of GK dimension one are (still) pi”, *Glasg. Math. J.* **45**:2 (2003), 243–247. [MR](#) [Zbl](#)
- [Paz 1984] A. Paz, “An application of the Cayley–Hamilton theorem to matrix polynomials in several variables”, *Linear Multilin. Algebra* **15**:2 (1984), 161–170. [MR](#) [Zbl](#)
- [Radjavi and Rosenthal 2000] H. Radjavi and P. Rosenthal, *Simultaneous triangularization*, Springer, 2000. [MR](#) [Zbl](#)
- [Sanz et al. 2010] M. Sanz, D. Pérez-García, M. M. Wolf, and J. I. Cirac, “A quantum version of Wielandt’s inequality”, *IEEE Trans. Inform. Theory* **56**:9 (2010), 4668–4673. [MR](#) [Zbl](#)

Communicated by Victor Reiner

Received 2018-11-14 Revised 2019-03-06 Accepted 2019-05-14

yaroslav-shitov@yandex.ru

Moscow, Russia

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Richard E. Borcherds	University of California, Berkeley, USA	Martin Olsson	University of California, Berkeley, USA
Antoine Chambert-Loir	Université Paris-Diderot, France	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	University of California, Santa Cruz, USA	Michael Rapoport	Universität Bonn, Germany
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Christopher Skinner	Princeton University, USA
Wee Teck Gan	National University of Singapore	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Andrew Granville	Université de Montréal, Canada	J. Toby Stafford	University of Michigan, USA
Ben J. Green	University of Oxford, UK	Pham Huu Tiep	University of Arizona, USA
Joseph Gubeladze	San Francisco State University, USA	Ravi Vakil	Stanford University, USA
Roger Heath-Brown	Oxford University, UK	Michel van den Bergh	Hasselt University, Belgium
Craig Huneke	University of Virginia, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Philippe Michel	École Polytechnique Fédérale de Lausanne	Melanie Matchett Wood	University of Wisconsin, Madison, USA
Susan Montgomery	University of Southern California, USA	Shou-Wu Zhang	Princeton University, USA
Shigefumi Mori	RIMS, Kyoto University, Japan		

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor


See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2019 is US \$385/year for the electronic version, and \$590/year (+\$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2019 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 13 No. 6 2019

Positivity functions for curves on algebraic varieties	1243
BRIAN LEHMANN and JIAN XIAO	
The congruence topology, Grothendieck duality and thin groups	1281
ALEXANDER LUBOTZKY and TYAKAL NANJUNDIAH VENKATARAMANA	
On the ramified class field theory of relative curves	1299
QUENTIN GUIGNARD	
Blow-ups and class field theory for curves	1327
DAICHI TAKEUCHI	
Algebraic monodromy groups of l -adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$	1353
SHIANG TANG	
Weyl bound for p -power twist of $\mathrm{GL}(2)$ L -functions	1395
RITABRATA MUNSHI and SAURABH KUMAR SINGH	
Examples of hypergeometric twistor \mathcal{D} -modules	1415
ALBERTO CASTAÑO DOMÍNGUEZ, THOMAS REICHELT and CHRISTIAN SEVENHECK	
Ulrich bundles on K3 surfaces	1443
DANIELE FAENZI	
Unlikely intersections in semiabelian surfaces	1455
DANIEL BERTRAND and HARRY SCHMIDT	
Congruences of parahoric group schemes	1475
RADHIKA GANAPATHY	
An improved bound for the lengths of matrix algebras	1501
YAROSLAV SHITOV	